The University of Western Ontario
London Canada

Department of Computer Science

Computer Science 9616a – Database Security and Privacy

Take-home, Part 1

Due: Oct. 28, 2015 at 3:30 p.m.

Please hand this in on paper, typed or written neatly.

You are expected to work alone on these questions.

1. (Basic Concepts) (8 marks) Answer two of the following:

   (a) Expolain why a Trojan horse program would be considered a bad thing.

   (b) Give 2 examples of security policies (not DAC or MAC, but rules about what people should be allowed to do) that might be required of a large system, and who would specify them.

   (c) DAC is "managed" by owners, which we could called decentralized, and MAC is managed by a security officer, which we could call centralized. What would be a good management strategy for access control in a large business? Briefly justify your answer.

2. (DAC for relations) (10 marks)

   Consider the following relation for a relational database:

   Appointments(PatientID, PatientName, Date, Time, PrimaryDoctor)

   Alice has created this table and has not given anyone any permissions on it.

   (a) What permissions does Alice have on this table?

   (b) Alice grants the Select permission to Bob on this table with grant option, then Bob grants Select to Carol. Can Bob now grant Select to Dave? Can Bob grant Insert to Dave?

   (c) How can Alice grant Select on a subset of the columns, say PatientName, Date, Time, to someone else?

   (d) How can Alice grant Select on a subset of the rows, say those patients whose PrimaryDoctor is "Dr. Bob", to someone else?

3. (MAC for relations) (22 marks)

Consider the following table for the Seaview model (this is the TS-instance); the key for the underlying relation is {PatID, Diagnosis}:

PatID	C_{PatID}	Diagnosis	$C_{Diagnosis}$	Doctor	C_{Doctor}	TC
123	U	AIDS	U	J. Smith	C	C
234	C	H1N1	C	G. D'Cunha	C	C
256	C	typhoid	C	B. Obama	C	S
344	C	mumps	C	J. Smith	S	S
344	S	H1N1	S	J. Smith	S	S
321	S	pneumonia	S	G. Bush	S	S

(a) Show the U-instance, C-instance and the S-instance of the above relation.

(b) Can the relation scheme for this relation be classified as C? Why or why not?

(c) Can the following tuple be inserted into the above relation? If not, give a reason (cite the property which is violated).
(321, S, pneumonia,TS, P. Martin, TS, TS)

(d) Can the following tuple be inserted into the above relation? If not, give a reason (cite the property which is violated).
(234, C, H1N1, C, G. Bush, C, C)

(e) Can the following tuple be inserted into the above relation? If not, give a reason.
(321, TS, pneumonia, TS, J. Smith, S, TS)

(f) Can the following tuple be inserted into the above relation? If not, give a reason (cite the property which is violated).
(344, S, flu, S, P. Martin, TS, TS)

(g) Can the following tuple be inserted into the above relation? If not, give a reason (cite the property which is violated).
(256, U, typhoid, U, J. Smith, U, U)

(h) Is there an example of polyinstantiation in your answers to parts(c) - (g)?

(i) Suppose there is also a relation Doctor, which gives the name, address, specialty etc. of Doctors. What does the Multilevel Referential Integrity property say about what tuples must exist in the relation Doctor, for the initial relation shown above?

4. (RBAC) (16 marks)

   (a) Construct a role graph for the following situation:

   We have the following regular roles: Office Mgr, Doctor, Nurse, Clerk.

   The Doctor can read and write PRecords, read and write Perscriptions and read Appointments.

   The Nurse can read PRecords, read Perscriptions, perform Tests.

   The Office Mgr can read and write Appointments, and read and write Accounts.

   The Clerk can read and write Appointments.

   Make sure that your role graph has the following role graph properties:

   - There is a single MaxRole.
   - The Role Graph is acyclic.
   - For any two roles r_i and r_j, if $r_i.rpset \subset r_j.rpset$, then there must be a path from r_i to r_j.

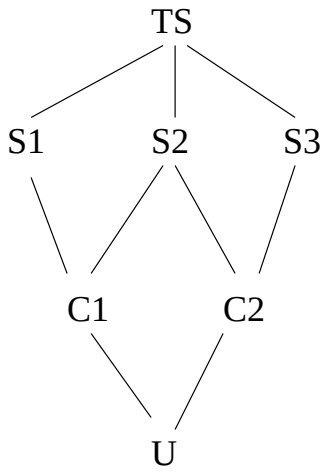
   (b) For each role in your role graph, list the direct and effective (union of direct and inherited) privileges.

   (c) We decide to add the privilege (Tests, perform) to role Doctor. What other change(s), if any, result from this privilege addition, assuming the role graph properties are to be maintained?

   (d) Going back to the original graph, suppose we decide to add the role LabTechnician to the role graph, with permissions to perform tests and read and write appointments. What is the result of this role addition (show the resulting role graph)?

5. (Comparison of Models) (15 marks)

We are trying to achieve MAC-like access control in an RBAC setting with the following lattice of security levels:



(a) Show the role hierarchy produced by the construction in Set 3, page 33 for the liberal $\star$-property.

(b) For a user cleared at S2, what roles would they be assigned to using this construction?

(c) For a user cleared at S2, what roles would they be able to activate in a session?

(d) For this S2 user, what permissions would they have, in a session (i.e. explain what permissions are available through the roles in your answer to (c).

(e) Follow the pattern of the role hierarchy for the strict $\star$-property shown on page 35 of Set 3. Draw the role hierarchy corresponding to this method for the above lattice. Assuming the strict $\star$-property, what role(s) would a user cleared at S2 be assigned to, and what permissions would be available to this S2 user by activating this (these) role(s)?

(f) If we were to create an additional role for the hierarchy constructed in part (a), say one which contained permissions to read items labeled S2, and write C1 and C2, can this role be assigned to anyone without violating the liberal $\star$-property?

(g) If we were to create an additional role for the hierarchy constructed in part (a), say one which contained permissions to read items labeled S1, and write C1 and C2, can this role be assigned to anyone without violating the liberal $\star$-property?